Akin®

Many More Defense Contractors Now Eligible for DoD Cyberthreat Info-Sharing Program

April 2, 2024

Reading Time : **3 min**

By: Natasha G. Kohne, Angela B. Styles, Michael J. Vernick, Joseph Hold

On March 12, 2024, the Department of Defense (DoD) finalized a rule to open its Defense Industrial Base (DIB) Cybersecurity (CS) Program to all defense contractors who own or operate an unclassified information system that processes, stores or transmits covered defense information.[1] This will allow said contractors to benefit from the DIB CS Program bilateral information sharing arrangement to keep informed about impending cyberthreats.

The new rule takes effect April 11, 2024.

Background

The DIB refers to the government, the DoD and the private sector industrial complex capable of researching, designing, developing, producing and maintaining military weapons systems to meet military requirements.[2] The DIB CS Program is a voluntary information sharing program to strengthen cybersecurity for DoD information transiting on, or residing on, DIB unclassified information systems.[3]

The DoD has mandatory cybersecurity activities contractually required through DFARS 252.204-7012.[4] The DIB CS Program's voluntary cyberthreat info-sharing is meant to bolster these activities, and also plays a key role in helping the DoD meet its critical infrastructure protection duties (see our prior post covering critical infrastructure protection in the Biden Administration's 2023 Cybersecurity Strategy).[5] The current DIB CS Program's objectives are:

- Establishing a voluntary, mutually acceptable framework for protecting information from unauthorized access;
- Protecting the confidentiality of information exchanged to the greatest extent permitted by law; and
- Creating a trusted environment to maximize network defense and remediation by both sharing cyberthreat information and incident reports, and providing mitigation and remediation strategies along with malware analysis.[6]

For eligible defense contractors, the DIB CS Program supports two-way information sharing and provides companies with the ability to access classified government information on cyberthreats targeting their networks and systems.[7]

The New Expanded Program

Eligibility for the DIB CS program is currently based on the October 2016 rule, which requires companies to be cleared defense contractors[8] who: (i) have DoD-approved medium assurance certificates; (ii) have an existing facility clearance to at least the Secret Level and (iii) can execute the standardized Framework Agreement[9]provided to interested contractors after verification that the company is eligible.[10]Due to multiple factors, namely the eligibility gap and the feedback from ineligible defense contractors, coupled with "a vulnerable DoD supply chain, and a pervasive cyber threat" the DoD is opening the DIB CS program up to non-cleared defense contractors.[11]Under the new expanded DIB CS Program, all defense contractors owning or operating an unclassified information system that processes, stores or transmits covered defense information will be eligible to participate in the program.

Impact of the Expansion

The DoD estimates that an additional 68,000 defense contractors will now be eligible for the DIB CS Program (currently only around 1,000 are participating).[12]Defense contractors that participate in the program will have access to technical exchange meetings, a collaborative web platform and threat information products and services through the DoD Cyber Crime Center (DC3). The DC3 shares cyber threat information and intelligence with the DIB, while also offering a range of tools, products, services and events for participants to benefit from.[13]

This expansion will enable many more smaller-sized defense contractors to take advantage of the DIB CS Program information sharing. The DoD emphasized that due to smaller contractors having fewer resources to devote to cybersecurity, leaving them out of the cyberthreat loop might create vulnerabilities that bad actors can exploit to gain national security information.[14]This expansion helps the defense contractor community at large better hone its cybersecurity capabilities.

---

[1] Department of Defense (DoD) Defense Industrial Base (DIB) Cybersecurity (CS) Activities, 89 Fed. Reg. 17741 (March 12, 2024) (to be codified at 32 C.F.R. pt. 236).

[2] *Id.* at 17742.

[3] *Id.*

[4] "Safeguarding Covered Defense Information and Cyber Incident Reporting" – https://www.ecfr.gov/current/title-48/chapter-2/subchapter-H/part-252/subpart-252.2/section-252.204-7012

[5] 89 Fed. Reg. 17742.

[6] *Id.*

[7] *Id.*

[8] A "cleared defense contractor" refers to a contractor cleared under the National Industrial Security Program (NISP) who has classified contracts with the DoD (32 C.F.R. 236.2).

[9] This Framework Agreement is made available after submitting an application on the program portal: https://dibnet.dod.mil/dibnet/.

[10] 89 Fed. Reg. 17743.

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] *Id.*

Categories

Cybersecurity, Privacy & Data Protection

Cybersecurity & Information Security

© 2024 Akin Gump Strauss Hauer & Feld LLP. All rights reserved. Attorney advertising. This document is distributed for informational use only; it does not constitute legal advice and should not be used as such. Prior results do not guarantee a similar outcome. Akin is the practicing name of Akin Gump LLP, a New York limited liability partnership authorized and regulated by the Solicitors Regulation Authority under number 267321. A list of the partners is available for inspection at Eighth Floor, Ten Bishops Square, London E1 6EG. For more information about Akin Gump LLP, Akin Gump Strauss Hauer & Feld LLP and other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.